UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

STEVEN JEFFREY HOWITT, on behalf of himself and all others similarly situated, Plaintiff, vs. CAPITAL ONE FINANCIAL CORPORATION, Defendant.	**COMPLAINT—CLASS ACTION** **Civil Action No.** **JURY DEMANDED**

Plaintiff, STEVEN JEFFREY HOWITT ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following against Defendant CAPITAL ONE FINANCIAL CORPORATION ("Capital One"), based upon his personal knowledge with respect to himself and his own acts, and upon information and belief, based upon his own investigation and the investigation of his counsel, as to all other matters, as follows:

SUMMARY OF ACTION

1. This is a class action brought by Plaintiff on behalf of himself and all other persons harmed by the cyberattack and breach of personal financial information ("Personal Information") maintained by Capital One on Amazon Web Services ("AWS") (the "Breach").

2. In a press release appended to a Form 8-K filed by Capital One on July 30, 2018 (the "July 30th 8-K"), Capital One announced that it was the subject of a hack consisting of the unauthorized access by an outside individual who obtained certain types of Personal Information relating to persons who had applied for its credit card and to Capital One customers.

3. A Complaint for Violations of 18 U.S.C. §1030(a)(2), filed by the U. S. Attorney for the Western District of Washington on July 29, 2019 (the "Criminal Complaint"), asserts that between March 12, 2019 and July 17, 2019, Paige A. Thompson ("Thompson"), a former employee of AWS, intentionally accessed a computer to obtain the information belonging to Capital One, and that Capital One learned of this potential hack on July 17, 2019.

4. According to the Criminal Complaint, Thompson was able to hack into Capital One's data base because of a firewall misconfiguration that permitted commands to reach and be executed by the server which maintained the hacked information, thereby enabling the hacker to gain access to folders or buckets of data in Capital One's storage place at AWS.

5. Capital One learned of the attack on July 17th, through an email from a previously unknown person, which contained certain commands, which when tested, provided access to over 700 buckets of customer information that Capital One maintains on AWS's servers.

6. As the Criminal Complaint asserts, the data copied from Capital One's data folders or buckets consists primarily of data related to credit card applications, including applicants' names, addresses, dates of birth and information regarding their credit history, which Capital One failed to tokenize or encrypt. It also contains approximately 120,000 social security numbers and approximately 77,000 bank account numbers.

7. Thompson subsequently posted about the theft on GitHub and on April 21, 2019, and leaked a list of more than 700 folders or buckets, as well as commands that enabled users to reach Capital One's date stored on AWS's servers. Capital One subsequently determined that a List Buckets Command was executed on April 21, 2019, and that it had evidence of that in its computer logs.

8. Its investigation further showed that Thompson had made several earlier attempts in March to obtain this information and to take advantage of the misconfigured firewall, but that Capital One did not recognize this suspicious activity. Criminal Comp. ¶13.

9. The data breach is one of the largest in history, as the Personal Information likely contains data for tens of millions of credit card applicants in the United States and Canada, exposing potential Class Members to damage.

10. Capital One chief executive officer, Richard Fairbank, has issued an apology, and as compensation for this breach and Capital One's apparent neglect in the maintenance of its firewall and in identifying Thompson's suspicious activity, has offered users and Class members complimentary credit monitoring and identity protection services. Neither of these can compensate Plaintiff and Class members for the increased risk of identity theft, and fraud which could occur as a consequence of the loss of this information.

11. By way of this action ("Action"), Plaintiff seeks to recover compensation to Class members for their risk and other damage which they have and will continue to suffer as a consequence of the Breach.

Parties

12. Plaintiff is a resident of New York, and applied for and maintained a Capital One credit card during the affected period.

13. Defendant Capital One is a Delaware corporation with a principal place of business in McLean Virginia. It is a bank holding company that specializes in credit cards, but also offers other credit, including automobile loans, as well as a variety of bank accounts.

Jurisdiction and Venue

14. This Court has jurisdiction over this Action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of costs and interest. At least one member of the putative Class is a citizen of a state different from that of the Defendant. There are more than 100 putative Class members.

15. This Court has personal jurisdiction over Capital One because does business here and this is the place in which the cause of action arose. Capital One provides credit card services throughout the United States, and, as such, has continuous and systematic contact with New York sufficient to provide it with the minimum contacts necessary to satisfy the principles of fair play and substantial justice and requirements of New York's long arm statute. Capital One has further committed a tortious act within this State. Capital One has purposefully availed itself of the law of New York.

16. Venue is proper in this judicial district pursuant to 28 U.S.C. §1391(a) because Capital one has committed a tortious act here, and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in this judicial district.

Class Action Allegations

17. Plaintiff brings this class action pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of himself and all others similarly situated who used applied for and/or maintained a credit card with Capital One from the period of 2005 to April 2019, and suffered damage or will suffer damage as a result of the Breach. Excluded from the Class is Defendant, any subsidiary, affiliate, parent, division or subdivision of the Defendant, and any employee or agent of Defendant.

18. The Class consists of approximately tens of millions of persons. As such, its members are so numerous that joinder is impracticable.

19. Questions of law and fact common to all members of the Class predominate, including:

a. whether Capital One acted negligently and/or wrongfully by failing to properly safeguard Plaintiff's and Class members' Personal Information;

b. whether Capital One failed to give timely and adequate notice of the Breach;

c. whether Capital One's conduct violated the law; and

d. whether Plaintiff and the other Class members have been damaged, and, if so, the relief that is appropriate.

20. Plaintiff's claims, as described herein, are typical of the claims of other Class members as Plaintiff's claims and those of other Class members arise from the same set of facts regarding Capital One's failure to protect Plaintiff's and Class members' private, Personal Information. Plaintiff maintains no interests antagonistic to the interests of other Class members.

21. Plaintiff is committed to the vigorous prosecution of this Action and has retained competent counsel experienced in the prosecution of class actions of this type.

22. Accordingly, Plaintiff is an adequate representative of the Class and will fairly and adequately protect its interests.

23. This class action is a fair and efficient method of adjudicating the claims of Plaintiff and Class members for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class members;

b. the prosecution of separate actions by individual members of the

Class would create a risk of inconsistent or varying adjudications with respect to individual Class members, thereby establishing incompatible standards of conduct for Defendant, or would allow the claims of some Class members to adversely affect the claims of other Class member, thereby affecting their ability to protect their interests; and

c. this forum is appropriate for litigation of this Action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this judicial district.

24. Plaintiff anticipates no difficulty in the management of this litigation as a class action, as the Class is readily definable, and its prosecution as a class action will eliminate the possibility of repetitious litigation, while providing redress for claims that may be too small to support the expense of individual, complex litigation.

25. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

Substantive Allegations

26. As a financial institution, Capital One has publicly stated that safeguarding its customers' information is essential to its mission and that it has invested heavily in cybersecurity.

27. Its current privacy policy ("Privacy Policy") specifically represents to its customers that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal laws. These measures include computer safeguard and secured files and buildings."

28. Despite this representation and its duties as a financial institution, due to its negligence, Capital One left itself vulnerable to a hack of critical, confidential customer information.

29. On July 30, 2018, Capital One for the first time announced that it had been hacked, and that critical customer information residing at servers maintained by AWS, had been stolen by a former AWS software engineer.

30. Thompson, the engineer, had posted the fact that she had stolen the information as early as April 2019. Moreover, she had made several attempts to hack Capital One's information throughout March 2019.

31. Nonetheless, Capital One failed to discover both Thompson's efforts, and the hack until a previously unknown tipster emailed Capital One and informed it of the hack on July 17, 2019.

32. Although Capital One knew since that time of the hack, it did not publicly admit to the hack nor did it inform customers of the hack until July 30, 2019.

33. Moreover, it informed customers of the through social media and two Form 8-K filings with the SEC on July 30th.

34. The cause of the hack, as announced thus far, is Capital One's failure to properly maintain its firewall for information that resides on the servers of AWS, and its failure to encrypt certain of the sensitive information. Capital One further failed to timely inform its customers of the hack, only doing so on July 30th by way of what many potential Class members believe is an ambiguous and vague email.

35. The Breach is one of the largest in history, as the hacked information likely contains data for tens of millions of credit card applicants in the United States and Canada, exposing potential Class Members to damage.

36. Capital One chief executive officer, Richard Fairbank, has issued an apology, and as compensation for this breach, and Capital One's apparent neglect in the maintenance of its

firewall and in identifying Thompson's suspicious activity, has offered users and Class members complimentary credit monitoring and identity protection services, neither of which can compensate Plaintiff and Class members for the increased risk of identity theft, and fraud which could occur as a consequence of the loss of this information.

37. The New York Attorney General's office has announced that it is launching an investigation into the Breach. The New York Department of Finance has reiterated that it will use all of its tools to protect New Yorkers.

PLAINTIFF'S ALLEGATIONS

38. Plaintiff applied for a Capital One card in about 2011 and has maintained a Capital One card since about early 2012.

39. In applying for his card, Plaintiff provided Capital One with his Personal Information, including his name, address, gender, birthdate, email address, credit card information and billing address—sufficient information from which a hacker could replicate his identity.

40. Plaintiff was unaware of the Breach until July 30th and therefore failed to take steps to protect himself from the Breach.

DAMAGES

41. Although Capital One has offered limited identity theft protection and indicated that it will be vigilant in monitoring Plaintiff's account for fraud, these efforts are insufficient to offset the risk to Plaintiff and Class members as a consequence of the Breach.

42. According to the U.S. Department of Justice, victims of identity theft have had, among other things, bank accounts wiped out, credit histories ruined, and jobs and valuable possessions taken away. In some cases, they have even been arrested for crimes committed by others using their name. The financial toll exacted by identity theft can be crippling, and the

emotional trauma can be devastating. A Federal Reserve Bank of Boston document states that identity thieves often use a stolen identity again and again and that it is very common for victims to learn that thieves have opened and accessed accounts spanning several years.

43. For the rest of their lives, Plaintiff and Class members will be forced to spend additional hours maintaining heightened diligence of their bank and card accounts, tax returns, etc., for fear of acts of identity theft against them and their families.

44. The damages, ascertainable losses and injuries, which have been and will be suffered by Plaintiff and the Class as a direct result of Capital One's violations of law, include, without limitation: (a) theft of their private Personal Information (b) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts after the limited monitoring being provided by Capital One; (c) loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they are permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations; (d) costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate and mitigate the actual and future consequences of the Breach, including without limitation, finding fraudulent charges, cancelling and reissuing cards, addressing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Breach; and (e) the imminent and certainly impending injury flowing from potential fraud and identity theft.

COUNT I

NEGLIGENCE AGAINST DEFENDANT

45. Plaintiff incorporates all of the preceding allegations as if fully set forth herein.

46. Capital One owed a duty to Plaintiff and other Class members to exercise reasonable care in obtaining, retaining, sharing, securing, safeguarding, and deleting their private, Personal Information and protecting that information from being compromised, lost, stolen and misused by an unauthorized person. They also owed Plaintiff and the Class a duty to timely disclose the Data Breach.

47. This duty included, among other things, designing, maintaining, updating, modernizing and testing its computer network and its interface with its partners, to ensure that Plaintiff's and Class members' personal, private information was adequately secured and protected, and to timely inform them, or any third party partner for whom Capital One acted as the search engine, of any breach.

48. Capital One further owed a duty to Plaintiff and Class members to implement processes in a timely manner that would detect a breach of its systems and prevent a mass export of users personal and private information.

49. Capital One owed a duty to Plaintiff and Class members to provide security consistent with industry standards, including ensuring that such private information was kept on secure. Its acts in failing to secure this information has created this relationship.

50. Plaintiff and Class members, who provided Capital One with their personal, private information were the foreseeable and probable victims of a data breach of Capital One's information.

51. Capital One was in a special relationship of trust with Plaintiff and Class members by being entrusted with their Personal Information. By reason of this special relationship, Capital One had a duty of reasonable care, which it unlawfully breached.

52. In the absence of negligence, Capital One would have known that its failure to properly construct its firewall and to detect potential hacking would cause damage to Plaintiff and other Class members and that it had a duty to adequately protect such information.

53. Plaintiff and Class members entrusted their private information to Capital One based upon their belief and understanding that Defendant would safeguard such information and had mechanisms available to protect such information from a data breach.

54. By negligently failing to take adequate steps to maintain their firewall and to detect the hacking, which made sensitive customer information vulnerable to attack, Capital One acted without reasonable due care and thereby breached their duties to Plaintiff and Class members.

55. Capital One's breach of their duty of due care, proximately caused damage and will continue to cause damage to Plaintiff and Class members.

56. Capital One committed this tortious act in violation of its Privacy Policy.

COUNT II

BAILMENT AGAINST DEFENDANT

57. Plaintiff incorporates all of the preceding allegations as if fully set forth herein.

58. Plaintiff and Class members provided their private, Personal Information to Capital One for the exclusive purpose of obtaining a credit card and using that card.

59. In delivering their private, Personal Information to Capital One, Plaintiff and Class members understood that Capital One would adequately safeguard this information. This was confirmed in Capital One's Privacy Policy.

60. Capital One accepted possession of Plaintiff's and other Class members' personal, private information for purposes of issuing a credit card and extending credit.

61. In accepting this information, Capital One understood that Plaintiff and other Class members expected Defendant to adequately safeguard their private information, as reflected in the Capital One Privacy Policy. Accordingly, a bailment was established for the mutual benefit of the parties.

62. During the bailment, Capital One owed a duty to Plaintiff and other Class members to exercise reasonable care, diligence and prudence in protecting their personal, private information.

63. As a direct and proximate cause of Capital One's breach of duty, Plaintiff and Class members suffered and will suffer consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages sought herein.

COUNT III

NEGLIGENCE PER SE AGAINST DEFENDANT

64. Plaintiff repeats and realleges each of the allegations stated above as if fully set forth herein.

65. Section 5 of the Federal Trade Commission Act, 15 U.S.C.§45, prohibits "unfair . . practices in or affecting commerce" including, the act of failing to use reasonable measures to protect Personal Information.

66. Capital One violated Section 5 of the FTC by failing to use reasonable measure to protect Personal Information and not complying with industry standards.

67. Capital One's violation of Section 5 of the FTC Act constitute negligence per se.

68. Class members are consumers within the class of persons that Section 5 of the FTC Act was intended to protect.

69. The harm caused by Capital One constitutes the type of harm that the FTC Act was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses for causing similar harm by failing to employ reasonable data security measures and avoid unfair and deceptive practices.

70. As a direct and proximate result of Capital One's negligence, Plaintiff and Class members have been injured and are entitled to damages.

COUNT IV

BREACH OF IMPLIED CONTRACT BY DEFENDANT

71. Plaintiff repeats and realleges each of the allegations above as if fully set forth herein.

72. In applying for credit at Capital One, Plaintiff and the other members of the Class entered into an implied contract with Defendant, whereby Defendants became obligated to reasonably safeguard Plaintiff's and the other Class members' Private Information.

73. Under the implied contract, Defendant was obligated to not only safeguard the Private Information, but also to provide Plaintiff and the other Class members with prompt, truthful, and adequate notice of any security breach or unauthorized access of said information.

74. Defendant breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their Private Information.

75. Defendant also breached its implied contract with Plaintiff and the other Class members by failing to provide prompt, truthful, and adequate notice of the Breach and unauthorized access of their Private Information by Thompson.

76. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) improper disclosure of their Private Information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Breach; (iii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud; (iv) the increased risk of identity theft; and (v) deprivation of the value of their Private Information, which is likely to be sold to cyber criminals on the dark web.

COUNT V

VIOLATION OF NEW YORK'S DATA BREACH LAWS – DELAYED NOTIFICATION AGAINST DEFENDANT
(N.Y. Gen. Bus. Law § 899-aa)

77. Plaintiff repeats and realleges each of the allegation above as if fully set forth herein.

78. Section 899-aa(3) of the New York General Business Law requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization."

79. The security breach notification shall be directly provided to the affected persons by: (a) written notice; (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business

relationship or engaging in any transaction; (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or (d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. N.Y. Gen. Bus. Law § 899-a(5).

80. The Breach described herein this Complaint constitutes a "breach of the security system" of Defendant.

81. As alleged above, Defendant unreasonably delayed informing Plaintiff and the and other Class members about the Breach, affecting the confidential and non-public Private Information of Plaintiff and other Class members after Defendants knew the Breach had occurred.

82. Defendant failed to disclose to Plaintiff and Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendant knew or reasonably believed such information had been compromised.

83. Defendant's ongoing business interests gave Defendant incentive to conceal the Breach from the public to ensure continued revenue.

84. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff and the Class members would impede Defendant's investigation.

85. As a result of Defendant's violation of New York law, Plaintiff and Class members were deprived of prompt notice of the Breach and were thus prevented from taking appropriate protective measures, including securing identity theft protection, or requesting a

credit freeze. These measures would have prevented some of the damages the Plaintiff and Class members suffered.

86. As a result of Defendant's violation of New York law, Plaintiff and Class members have suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

87. Plaintiff and Class members seek all remedies available under New York law, including, but not limited to damages as well as equitable relief.

PRAYER FOR RELIEF

Plaintiff, on behalf of himself and all others similarly situated, requests that the Court provide the following relief:

a. Certifying this Action as a Class action and appointing Plaintiff as an adequate representative of the Class, and his counsel as Class counsel;

b. Entering judgment, including pre-judgment and post-judgment interest, in favor of Plaintiff and the Class and against Defendant;

c. Awarding Plaintiff and Class members appropriate relief, including actual and statutory damages, restitution, disgorgement and, where appropriate, injunctive relief requiring Defendants to take steps to ensure against a recurrence of the Breach by adopting and implementing reasonable data security measures, among other things;

d. Awarding Plaintiff and Class members attorney's fees, expenses, and costs of this Action; and

e. Ordering such further and other relief as the Court deems necessary.

JURY DEMANDED

Plaintiff, individually and on behalf of the putative Class, demands trial by jury on all issues so triable.

Dated: July 31, 2019

THEGRANTLAWFIRM, PLLC

By: Lynda J. Grant

521 Fifth Avenue, 17th Floor
New York, NY 10175
T/212-292-4441
F/212-292-4442
E/lgrant@grantfirm.com

Attorneys for Plaintiff and the Class